

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-181898

(43)Date of publication of application : 30.06.2000

(51)Int.Cl.

G06F 15/78
G06F 12/14

(21)Application number : 10-354198

(71)Applicant : NEC CORP

(22)Date of filing : 14.12.1998

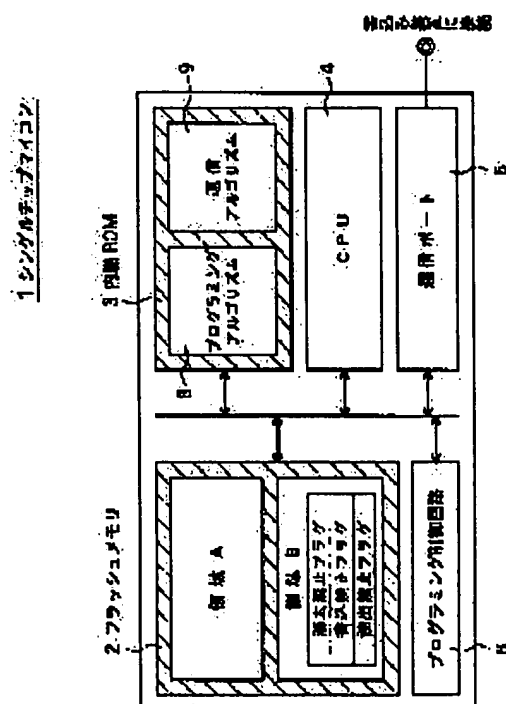
(72)Inventor : OKUDA IKUTARO

(54) FLASH MEMORY MOUNTED TYPE SINGLE CHIP MICROCOMPUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a single chip microcomputer which easily performs write, read and erase management to/from a flash memory about which security measures are considered and has a security function needed for copyright protection, etc.

SOLUTION: This single chip microcomputer 1 consists of a flash memory 2, a built-in ROM 3, a CPU 4, a communication port 5 and a programming controller 6. The memory 2 arranges an area A where programming is performed and an area B for designating a write flag, a read flag and an erase flag which are management information to the area A as pair areas. When a programming request comes from the outside, the CPU 4 refers to the management information of the area B and decides the propriety of executing programming of the area A.



LEGAL STATUS

[Date of request for examination] 18.03.1999

[Date of sending the examiner's decision of rejection] 12.09.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2002-20052

[Date of requesting appeal against examiner's decision of rejection] 15.10.2002

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-181898

(P2000-181898A)

(43) 公開日 平成12年6月30日 (2000.6.30)

(51) Int.Cl. ⁷	識別記号	F I	テマート* (参考)
G 0 6 F 15/78	5 1 0	G 0 6 F 15/78	5 1 0 A 5 B 0 1 7
12/14	3 1 0	12/14	3 1 0 F 5 B 0 6 2

審査請求 有 請求項の数 4 O L (全 6 頁)

(21) 出願番号 特願平10-354198

(22) 出願日 平成10年12月14日 (1998. 12. 14)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 奥田 郁太郎

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100096231

弁理士 稲垣 清

Fターム(参考) 5B017 AA02 AA03 BA04 BB02 BB03

CA12 CA13 CA15

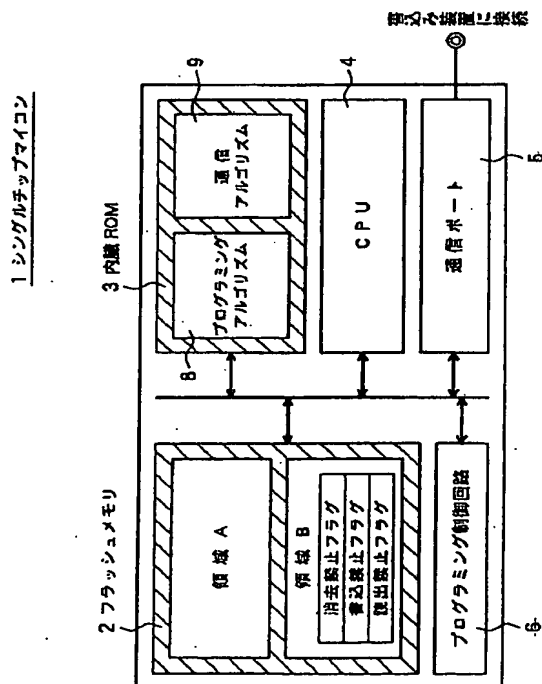
5B062 AA07 CC03 DD10

(54) 【発明の名称】 フラッシュメモリ搭載型シングルチップマイクロコンピュータ

(57) 【要約】

【目的】 セキュリティ対策が考慮されたフラッシュメモリへの書込み、読出し、及び、消去の管理を容易に行うことができ、著作権保護等のために必要なセキュリティ機能を有するシングルチップマイコンを提供する。

【構成】 シングルチップマイコン1は、フラッシュメモリ2と、内蔵ROM3と、CPU4と、通信ポート5と、及び、プログラミング制御回路6とで構成されている。フラッシュメモリ2は、プログラミングする領域Aと該領域Aへの管理情報である書込みフラグ、読出しフラグ、及び、消去フラグを指定するための領域Bとを対領域として配設する。CPU4は、外部からのプログラミング要求があると、前記領域Bの前記管理情報を参照して前記領域Aのプログラミングの実行の可否を判断する。



【特許請求の範囲】

【請求項1】 フラッシュメモリとマイクロプロセッサとを1の基板上に配設したシングルチップマイクロコンピュータにおいて、

前記フラッシュメモリに第1の領域と該第1の領域のプログラミングの可否を指定するための第2の領域とを配設し、前記マイクロプロセッサは、外部からのプログラミング要求があると、前記第2の領域を参照して前記第1の領域のプログラミングの実行の可否を判断することとを特徴とするシングルチップマイクロコンピュータ。

【請求項2】 前記マイクロプロセッサは、前記第1の領域にプログラミングを実行した際に、前記第1の領域のプログラミングを禁止する命令を前記第2の領域に書き込む、請求項1に記載のシングルチップマイクロコンピュータ。

【請求項3】 前記マイクロプロセッサは、前記フラッシュメモリのプログラミングアルゴリズムが記録された、シングルチップマイクロコンピュータ内蔵のROMによって、前記第2の領域を参照するように制御される、請求項1又は2に記載のシングルチップマイクロコンピュータ。

【請求項4】 前記マイクロプロセッサは、ローダプログラムが記録された、シングルチップマイクロコンピュータ内蔵のROMによって、前記第2の領域を参照するように制御される、請求項1又は2に記載のシングルチップマイクロコンピュータ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、フラッシュメモリを搭載したシングルチップマイクロコンピュータに関するものである。

【0002】

【従来の技術】フラッシュメモリとマイクロプロセッサとを1つのチップに組み込んだフラッシュメモリ搭載型シングルチップマイクロコンピュータ（以下、シングルチップマイコンと呼ぶ）が用いられている。従来のシングルチップマイコンについて、図3を参照して説明する。このシングルチップマイコン1は、フラッシュメモリ2と、通信ポート5と、CPU4と、内蔵ROM3と、及び、プログラミング制御回路6とから成る各機能部で構成されている。

【0003】フラッシュメモリ2は、この内部領域を任意の領域（A又はB）に分割して管理され、分割した各領域において書き込み、読出し、及び、一括消去の各動作が可能である。

【0004】通信ポート5は、フラッシュメモリ2に対して外部から書き込みを行う外部の書き込み装置と接続し、書き込みデータや専用コマンド等の情報をやり取りする。

【0005】CPU4は、シングルチップマイコン1の全体を管理し、内蔵ROM3やフラッシュメモリ2等の

プログラムに基づいた処理を実行する。

【0006】内蔵ROM3には、通信ポート5を介してやり取りした情報を受け渡すための手順を記述した通信アルゴリズム9と、フラッシュメモリ2の任意の領域への書き込み、読出し、及び、消去を行うための手順を記述したプログラミングアルゴリズム8とが予め格納されている。

【0007】プログラミング制御回路6は、CPU4の制御に基づいてフラッシュメモリ2への実際の書き込み、読出し、及び、消去の処理を実行する。

【0008】シングルチップマイコン1では、プログラミング専用の動作モードにおいて書き込み装置から専用コマンドが入力されると、CPU4がプログラミングアルゴリズム8中の手順に従ってプログラミング制御回路6を制御することによって、フラッシュメモリ2の任意の領域に対して書き込み、読出し、及び、一括消去が実行される。

【0009】従来のシングルチップマイコン1では、フラッシュメモリ2内の領域への書き込み、読出し、及び、消去のプログラミング動作は、専用コマンドで無制限に実行されるため、その実行については書き込み装置側に全ての権限が与えられ、フラッシュメモリ2上の情報に対してセキュリティ対策が考慮されていない。この場合、内蔵フラッシュメモリに既に格納されたプログラムの解析や改変等が行われ、ソフトウェアの著作権の保護ができない。

【0010】特開平4-17477号公報には、ICカードの制御に関する技術が記載されている。図4は、該公報に記載のICカードのデータ構成を示すブロック図である。マイクロコンピュータ21は内部メモリ25を有し、内部メモリ25には、バス線を介して端末装置28及び外部メモリ22との間で通信を実行する通信プログラム、通信時の情報が正しいか否かのチェックを行うチェックプログラム、及び、パスワード等の秘密保持を行う秘密保持プログラム等の基本処理プログラムが予め書き込まれている。さらに上記内部メモリ25のプログラム等によって必要な処理を実行するCPU24や、その他インターフェイスが設けられている。

【0011】マイクロコンピュータ21と並んで配設された外部メモリ22は、PROMとして構成され、ユーザの必要な処理を行うプログラムが自由に書き込めるユーザプログラムエリア26と、所望のデータを書き込むデータエリア27の2つのエリアを設定してある。

【0012】内部メモリ25には、外部メモリ22内のユーザプログラムエリア26のアドレスと、データエリア27の先頭及び最終のアドレスとが予め書き込まれている。従って、ユーザプログラムのロード完了時には、ユーザプログラムエリア26の最終アドレスにユーザプログラム書き込み終了のマークが設定される。

【0013】そのため、ユーザプログラムエリア26へ

のユーザプログラムの再ロードの禁止等は、ユーザプログラム書込み終了のマークの有無により行い、データエリア27への書込み及び読出しの禁止等は、パスワード機能やコードチェックや暗号化することをプログラムとして、ユーザプログラムエリア26中に作成することで実現していた。

【0014】

【発明が解決しようとする課題】上記公報に記載の内容は、一般的なIPL (Initial Program Loader) 機能について述べたものであり、初期的なパーソナルコンピュータで既に実現されているもので、著作権保護等のために必要なセキュリティ機能のために行うデータの扱い方や処理手段は明示されていない。

【0015】また、外部メモリ22にEEPROMを使用した場合には、ブロック単位で電氣的消去が可能となるが、上記シングルチップマイクロコンピュータでは、その電氣的な消去については記載がない。

【0016】本発明は、上記したような従来の技術が有する問題点を解決するためになされたものであり、セキュリティ対策が考慮されたフラッシュメモリへの書込み、読出し、及び、消去の管理を容易に行うことができ、著作権保護等のために必要なセキュリティ機能を有するシングルチップマイコンを提供することを目的とする。

【0017】

【課題を解決するための手段】上記目的を達成するため、本発明のシングルチップマイコンは、フラッシュメモリとマイクロプロセッサとを1の基板上に配設したシングルチップマイクロコンピュータにおいて、前記フラッシュメモリに第1の領域と該第1の領域のプログラミングの可否を指定するための第2の領域とを配設し、前記マイクロプロセッサは、外部からのプログラミング要求があると、前記第2の領域を参照して前記第1の領域のプログラミングの実行の可否を判断することを特徴とする。

【0018】本発明のシングルチップマイコンによると、書込みフラグ、読出しフラグ、消去フラグの各管理情報を参照することで、該フラッシュメモリへの書込み、読出し、消去の各動作に関する禁止や許可等の管理が容易に行える。

【0019】本発明のシングルチップマイコンの好ましい態様では、前記第1の領域にプログラミングを実行した際に、前記第1の領域のプログラミングを禁止する命令を前記第2の領域に書き込むことを特徴とする。

【0020】かかる構成により、プログラムの著作権保護やシステムの安全性保護等の観点から、内蔵のフラッシュメモリ上のソフトウェアの解析や改変を目的とした、フラッシュメモリへの意図的な書込み、読出し、及び、消去のプログラミング動作を任意に禁止できる。

【0021】前記マイクロプロセッサは、プログラミン

グの実行の可否を判断するアルゴリズムを、予め内蔵のROMに記録する構成を採用をすることも、或いは、そのようなアルゴリズムを、内蔵のROMに予め記録してあるローダプログラムに従って外部からロードする構成を採用をすることもできる。いずれの場合にもプログラミングの実行の可否を判断することが可能になる。

【0022】

【発明の実施の形態】次に、本発明のシングルチップマイコンが行う、セキュリティ対策が考慮されたフラッシュメモリへの書込み、読出し、及び、消去についての動作を図面を参照して説明する。図1は、本発明の第1の実施形態例のシングルチップマイコンのブロック図である。シングルチップマイコン1は、フラッシュメモリ2と、内蔵ROM3と、CPU4と、通信ポート5と、及び、プログラミング制御回路6とで構成される。

【0023】フラッシュメモリ2は予め領域Aと領域Bに分割され、領域Bは、領域Aの管理情報である消去禁止フラグと書込み禁止フラグと読出し禁止フラグとを有する。つまり、領域Aと領域Bは対領域として構成される。フラッシュメモリ2には、このような対領域が複数配設される。

【0024】内蔵ROM3は、通信ポート5を介してやり取りした情報を受け渡すための手順を記述した通信アルゴリズム9と、フラッシュメモリ2の任意の領域を書込み、消去するための手順を記述したプログラミングアルゴリズム8とが、格納されている。

【0025】CPU4は、シングルチップマイコン1を管理し実行する。通信ポート5は、外部の書込み装置と接続し書込みデータや専用コマンド等情報をやり取りする。プログラミング制御回路6は、CPU4の制御に基づいて、フラッシュメモリ2への実際の書込み、読出し、及び、消去の処理を実行する。

【0026】初期状態では、フラッシュメモリ2を構成する個々のメモリセルは消去状態である1を保持している。CPU4は、通信アルゴリズム9に従って、通信ポート5を介して外部の書込み装置との間で情報をやり取りする。CPU4は、書込み装置からの情報がフラッシュメモリ2の領域Aに対する書込み、読出し、又は、消去を指示するものである場合には、プログラミングアルゴリズム8に従い、領域Bの各フラグを参照してプログラミング制御回路6を制御して領域Aのためのプログラミング動作を行う。

【0027】プログラミングが消去動作である場合には、CPU4は領域Bの消去禁止フラグを参照し、禁止を示す0であれば消去動作を拒否し、許可を示す1であればプログラミングアルゴリズム8に従い、プログラミング制御回路6を制御して領域Aの消去動作を実行する。

【0028】プログラミングが書込み動作である場合には、CPU4は領域Bの書込み禁止フラグを参照し、禁

止を示す0であれば書込み動作を拒否し、許可を示す1であればプログラミングアルゴリズム8に従い、プログラミング制御回路6を制御して領域Aの書込み動作を実行する。

【0029】プログラミングが読出し動作である場合には、CPU4は領域Bの読出し禁止フラグを参照し、禁止を示す0であれば読出し動作を拒否し、許可を示す1であればプログラミングアルゴリズム8に従い、プログラミング制御回路6を制御して領域Aの読出し動作を実行する。

【0030】上記実施例によれば、フラッシュメモリへのプログラミング動作を、各領域毎に容易に禁止及び許可ができる。

【0031】図2は本発明のシングルチップマイコンの第2の実施形態例を示すブロック図である。本実施形態例のシングルチップマイコンは、内蔵RAM7を備える点において先の実施形態例とは異なる。

【0032】内蔵ROM3には、通信アルゴリズムとプログラミングアルゴリズムとを、通信ポート5経由で内蔵RAM7にダウンロードするための手順を記述したロードプログラム10が、予め格納されている。

【0033】初期状態では、フラッシュメモリ2を構成する個々のメモリセルは消去状態である1を保持している。CPU4は内蔵ROM3に予め格納されたロードプログラム10を実行し、通信ポート5経由で通信アルゴリズムとプログラミングアルゴリズムを内蔵RAM7にダウンロードする。その後、CPU4は内蔵RAM7に配置された通信アルゴリズム9に従って、通信ポート5を介して外部の書込み装置との間で情報をやり取りする。

【0034】CPU4は、その情報がフラッシュメモリ2の領域Aに対する書込み、読出し、及び、消去のプログラミング動作を指示する場合には、プログラミングアルゴリズムに従い、領域Bの各フラグを参照してプログラミング制御回路6を制御して領域Aのプログラミング動作を行う。書込み、読出し、及び、消去のプログラミング動作の実際については、第1の実施形態例と同様であるため、その説明を省略する。

【0035】内蔵ROM3は、一般にはマスクROMとして構成され、例えば製造後にアプリケーション等の関係でプログラミングアルゴリズム及び通信アルゴリズムを変更する等の場合に容易に対応できる。

【0036】また、上記の第1及び第2の実施形態例の

シングルチップマイコンは、上記のプログラミングアルゴリズムの他に、フラッシュメモリ2を全消去状態にできるテストモードを備える。このテストモードは、シングルチップマイコンの製品を出荷する際に、フラッシュメモリをデフォルトとして全消去する際に利用される。

【0037】

【発明の効果】フラッシュメモリに設定した領域単位で、書込み、読出し、及び、消去のプログラミング動作に関する禁止や許可等の管理を容易に実現することができるので、プログラムの改変や解析等による著作権の侵害を未然に防止できる。この場合、管理する領域単位での禁止や許可等の状態が明確であるため、複数に分割して管理することもできる。

【図面の簡単な説明】

【図1】本発明のシングルチップマイコンの第1の実施形態例を示すブロック図である。

【図2】本発明のシングルチップマイコンの第2の実施形態例を示すブロック図である。

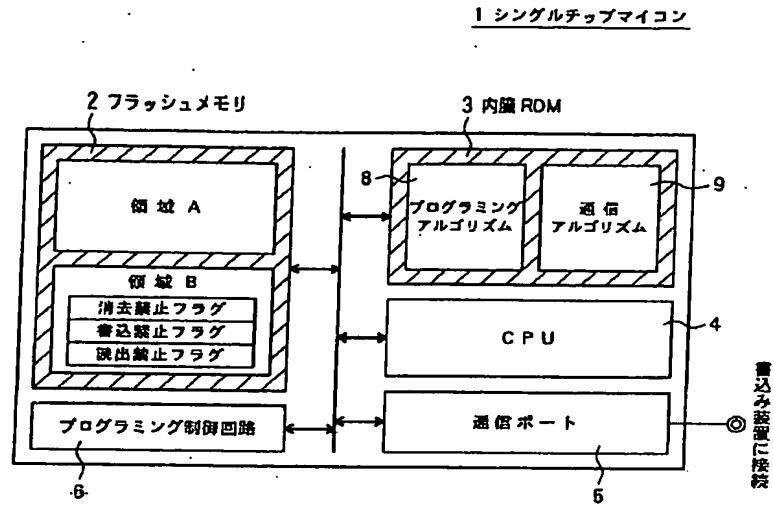
【図3】セキュリティ対策を装備しないシングルチップマイコンを示すブロック図である。

【図4】特開平4-17477号公報に記載のICカードのデータ構成を示すブロック図である。

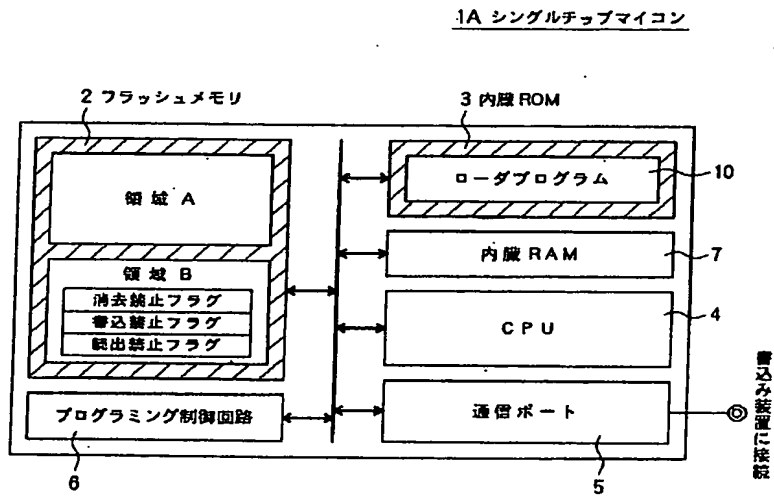
【符号の説明】

- 1 シングルチップマイコン
- 2 フラッシュメモリ
- 3 内蔵ROM
- 4 CPU
- 5 通信ポート
- 6 プログラミング制御回路
- 7 内蔵RAM
- 8 プログラミングアルゴリズム
- 9 通信アルゴリズム
- 10 ロードプログラム
- 20 ICカード
- 21 マイクロコンピュータ
- 22 外部メモリ
- 23 インターフェイス
- 24 CPU
- 25 内部メモリ
- 26 ユーザプログラムエリア
- 27 データエリア
- 28 端末装置

【図1】

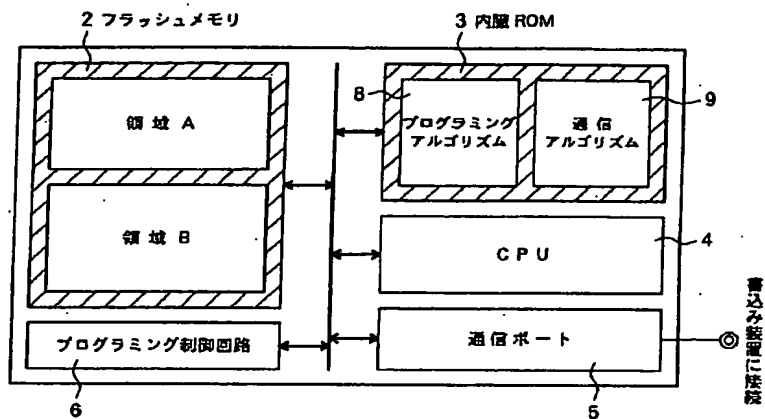


【図2】



【図3】

1 シングルチップマイコン



【図4】

